LECTURE 10

Type-1.

* Sample (A, T_A) s.t. $A \in \mathbb{Z}_q^{n \times m}$, $T \in \mathbb{Z}_q^{m \times m}$

$\longrightarrow A T_A = 0 \pmod q$

$\longrightarrow$ T has rank m over $\mathbb{Z}$.

$\longrightarrow$ T is "short".

Type-2.

Sample (A, T_{GA}) s.t.

$A T_{GA} = G$.

Trapdoor One-Way Functions.

KG $\longrightarrow$ "pk" or "ik" $= A$, "sk" $= T_A$

$f_A(s, e) \longrightarrow s^T A + e^T = b^T$

$f_A^{-1}(b, T_A) \longrightarrow$ Compute $y = b^T T_A = e^T T_A$

SOLVE for e.

ANOTHER TRAPDOOR FUNCTION.

(BASED ON SIS)

KeyGen $\rightarrow \left(B, T_{GB}\right)$ s.t. $BT_{GB} = G$.

Sample $\tilde{A} \leftarrow \mathbb{Z}_q^{n \times m}$

$R \leftarrow \{0,1\}^{m \times m \log q}$

$B = \left[\tilde{A} \,\|\, \tilde{A}R + G\right]$

$T_B = \begin{bmatrix} -R \\ I \end{bmatrix}$

KeyGen $(1^\lambda) \rightarrow B, T_{GB}$.

$f_B(e) \rightarrow Be \pmod q$

(e: "short")

$f_B^{-1}(v, T_{GB}) \rightarrow$ Given A, v find e s.t. $Ae = v$

Can you find some e' s.t. $Ge' = v$?

$\downarrow$ $\in \mathbb{Z}_q^{m \log q}$

$e' = G^{-1}(v)$.

T_{BG} s.t. $B T_{BG} = G$.

Can you now find e s.t. $Be = v$.

H.W. Find some $\hat{e}$ s.t. $Be = v$.]

SIS

Given A, v find "short" e s.t. $Ae = v$.

We discussed how to find a solution, but actually we need "nice" solutions.

DIGITAL SIGNATURE

$\text{KeyGen}(1^\lambda) \rightarrow vk, sk$

$\text{Sign}(m, sk; r) \rightarrow \sigma$

$\text{Verify}(\sigma, m, vk) \rightarrow 0/1$

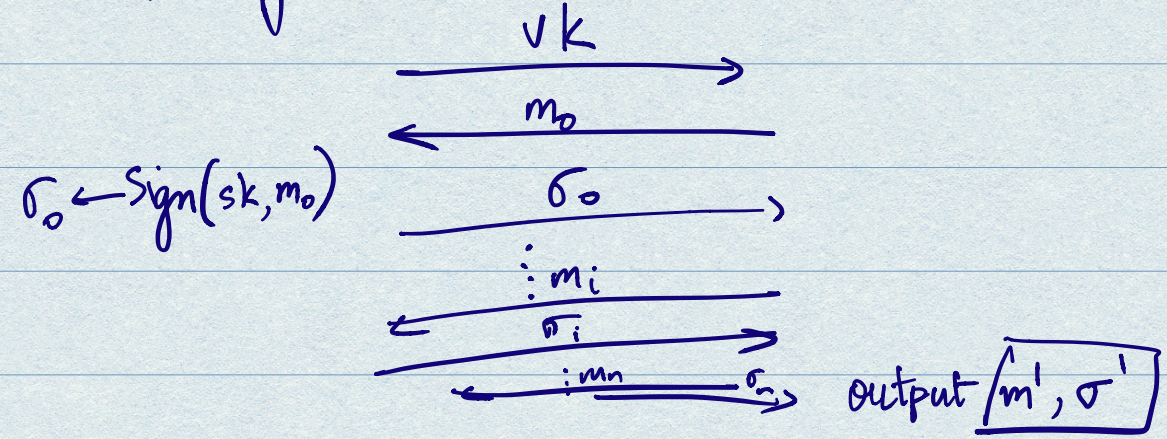
Correctness: $\forall m$, whp over (sk, vk, r)

$\text{Verify}(\text{Sign}(m, sk; r), m, vk) = 1$

Security:

Ch Adv

$(vk, sk) \leftarrow \text{KeyGen}$



A wins if

$$m' \notin \{ m_0 \ldots\ldots m_n \}$$

and

$$\text{Verify}(\sigma', m', vk) = 1$$

We say that a signature scheme (KeyGen, Sign, Verify) is secure if

$$\Pr_{(sk, vk) \leftarrow KG(1^\lambda)} [A \text{ wins}] = \text{negl}(\lambda)$$

Q: Build a Digital signature scheme whose security is based on the hardness of SIS.

KeyGen $(1^\lambda) \rightarrow A, T_A$

A = vk, T_A = sk

Sign $(m, \underset{= T_A}{sk}) \rightarrow$

Suppose we had a hash function

$H(m) \rightarrow v \in \mathbb{Z}_q^n$

Find "short" e (using T_A) s.t. $Ae = v$

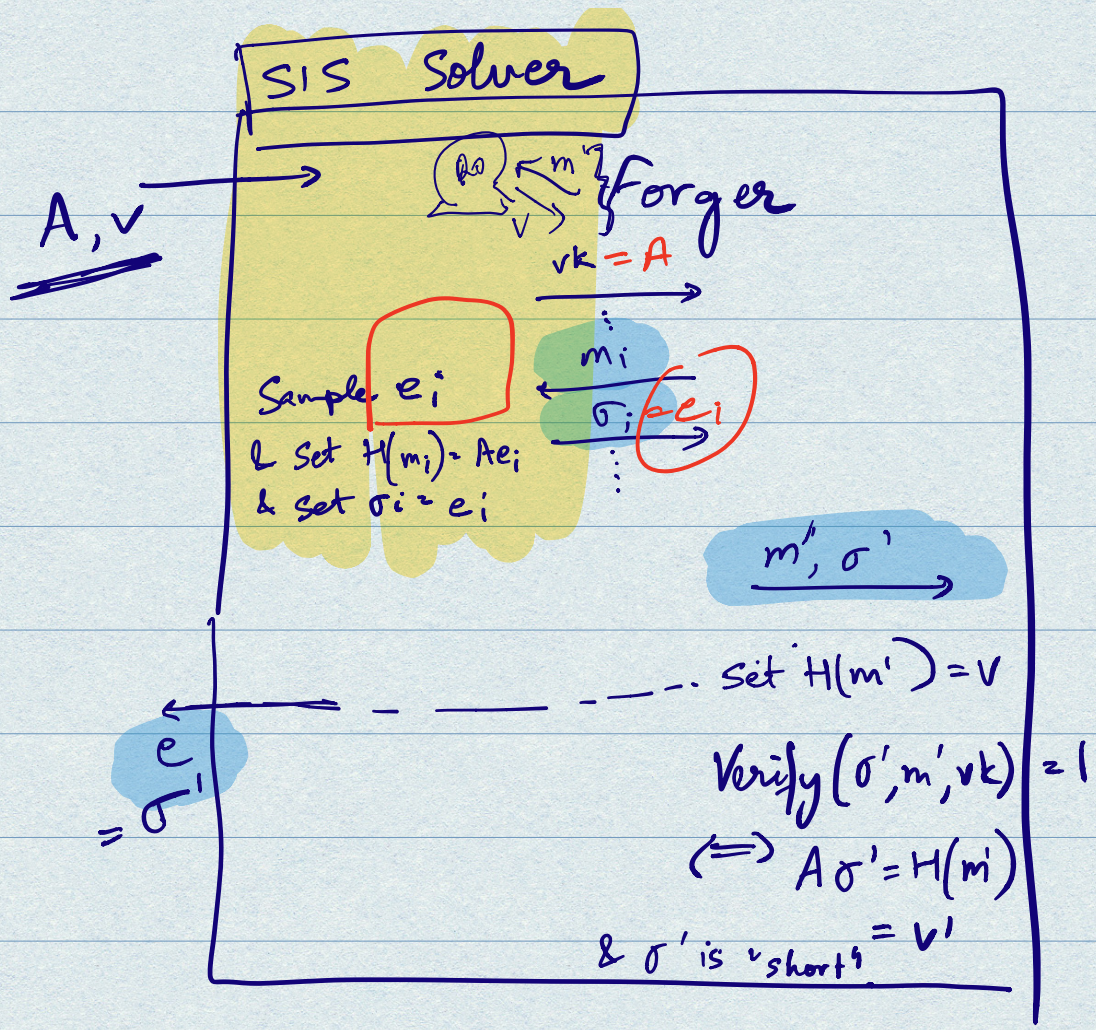
Verify $(\sigma, m, \underset{= A}{vk})$:

Check if $A\sigma = H(m)$

and σ is "short".

If checks pass, output 1.

Else, output 0.

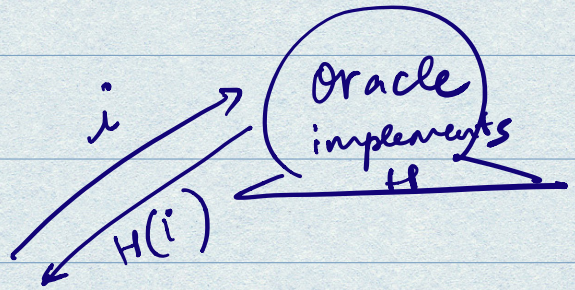


RANDOM ORACLE

Truly random function.

H is a random oracle.

RANDOM ORACLE

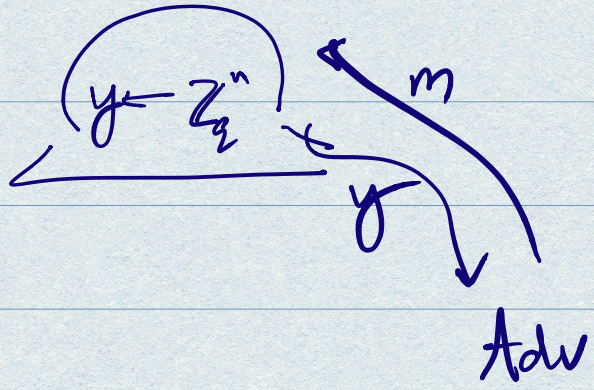


Alice Bob Adv.

To compute $H(i)$

On proofs.

"program" the random oracle



m_i

$v = H(m_i)$

To prove security of the Dig. Sign. scheme, we need a "special trapdoor SIS-solver".

$$\left(A \leftarrow \mathbb{Z}_q^{n \times m},\ e \leftarrow D_{\mathbb{Z}^m, s},\ v = Ae \bmod q \right)$$

(s: std. dev^n $= \|T_A\| \cdot \omega(\sqrt{\log n})$)

$$\approx_{\text{stat}}$$

$$\left(A \leftarrow \mathbb{Z}_q^{n \times m},\ v \xleftarrow{\$} \mathbb{Z}_q^m,\ \text{find } e \leftarrow \text{TrapSISSolve}(A, T_A, v) \right).$$

IDENTITY - BASED ENCRYPTION

A TA

KeyGen $(1^\lambda) \rightarrow mpk, msk$

Enc $(mpk, id, m; r) \rightarrow ct$

TA Compute $y = H(id)$, find e short s.t. $Ae = y$

SKGen $(msk, id) \rightarrow sk_{id}$

Dec $(ct, sk_{id'}) \rightarrow m$ if $id = id'$

ct = $(id \| ciphertext)$ $\perp$ otherwise

Given $sk_{id=1}, sk_{id=2} \ldots sk_{id=n}$,

should not be able to infer

sk_{id} for any $id \notin \{1, 2 \ldots n\}$

Given $\sigma_{m=1}, \sigma_{m=2} \ldots \sigma_{m=n}$, should not be able to compute $\sigma_{m'}$ for $m' \notin \{1, 2 \ldots n\}$